



## 97TH GENERAL ASSEMBLY

### State of Illinois

2011 and 2012

HB2053

by Rep. Darlene J. Senger

#### SYNOPSIS AS INTRODUCED:

720 ILCS 5/16D-2

from Ch. 38, par. 16D-2

720 ILCS 5/16D-3

from Ch. 38, par. 16D-3

Amends the Criminal Code of 1961. Provides that a person commits the offense of computer tampering when knowingly, and without the authorization of a computer's owner, engages in electronic hi-jacking, or sends false data such as information, pictures, or videos as the owner of a hi-jacked account. Defines electronic hi-jacking as a network security attack in which the attacker takes unauthorized control of electronic communications, social networking sites, computer networks or programs of another. Provides that a first offense is a Class 4 felony and a second or subsequent offense is a Class 3 felony.

LRB097 02970 RLC 42995 b

1 AN ACT concerning criminal law.

2 **Be it enacted by the People of the State of Illinois,**  
3 **represented in the General Assembly:**

4 Section 5. The Criminal Code of 1961 is amended by changing  
5 Sections 16D-2 and 16D-3 as follows:

6 (720 ILCS 5/16D-2) (from Ch. 38, par. 16D-2)

7 Sec. 16D-2. Definitions. As used in this Article, unless  
8 the context otherwise indicates:

9 (a) "Computer" means a device that accepts, processes,  
10 stores, retrieves or outputs data, and includes but is not  
11 limited to auxiliary storage and telecommunications devices  
12 connected to computers.

13 (a-5) "Computer network" means a set of related, remotely  
14 connected devices and any communications facilities including  
15 more than one computer with the capability to transmit data  
16 among them through the communications facilities.

17 (b) "Computer program" or "program" means a series of coded  
18 instructions or statements in a form acceptable to a computer  
19 which causes the computer to process data and supply the  
20 results of the data processing.

21 (b-5) "Computer services" means computer time or services,  
22 including data processing services, Internet services,  
23 electronic mail services, electronic message services, or

1 information or data stored in connection therewith.

2 (c) "Data" means a representation of information,  
3 knowledge, facts, concepts or instructions, including program  
4 documentation, which is prepared in a formalized manner and is  
5 stored or processed in or transmitted by a computer. Data shall  
6 be considered property and may be in any form including but not  
7 limited to printouts, magnetic or optical storage media, punch  
8 cards or data stored internally in the memory of the computer.

9 (c-5) "Electronic mail service provider" means any person  
10 who (1) is an intermediary in sending or receiving electronic  
11 mail and (2) provides to end-users of electronic mail services  
12 the ability to send or receive electronic mail.

13 (d) In addition to its meaning as defined in Section 15-1  
14 of this Code, "property" means: (1) electronic impulses; (2)  
15 electronically produced data; (3) confidential, copyrighted,  
16 or proprietary information; (4) private identification codes  
17 or numbers which permit access to a computer by authorized  
18 computer users or generate billings to consumers for purchase  
19 of goods and services, including but not limited to credit card  
20 transactions and telecommunications services or permit  
21 electronic fund transfers; (5) software or programs in either  
22 machine or human readable form; or (6) any other tangible or  
23 intangible item relating to a computer or any part thereof.

24 (e) "Access" means to use, instruct, communicate with,  
25 store data in, retrieve or intercept data from, or otherwise  
26 utilize any services of a computer.

1           (f) "Services" includes but is not limited to computer  
2 time, data manipulation, or storage functions.

3           (g) "Vital services or operations" means those services or  
4 operations required to provide, operate, maintain, and repair  
5 network cabling, transmission, distribution, or computer  
6 facilities necessary to ensure or protect the public health,  
7 safety, or welfare. Those services or operations include, but  
8 are not limited to, services provided by medical personnel or  
9 institutions, fire departments, emergency services agencies,  
10 national defense contractors, armed forces or militia  
11 personnel, private and public utility companies, or law  
12 enforcement agencies.

13           (h) "Social networking website" means an Internet website  
14 containing profile web pages of the members of the website that  
15 include the names or nicknames of such members, photographs  
16 placed on the profile web pages by such members, or any other  
17 personal or personally identifying information about such  
18 members and links to other profile web pages on social  
19 networking websites of friends or associates of such members  
20 that can be accessed by other members or visitors to the  
21 website. A social networking website provides members of or  
22 visitors to such website the ability to leave messages or  
23 comments on the profile web page that are visible to all or  
24 some visitors to the profile web page and may also include a  
25 form of electronic mail for members of the social networking  
26 website.

1        (i) "Electronic hi-jacking" means a network security  
2 attack in which the attacker takes unauthorized control of  
3 electronic communications, social networking sites, computer  
4 networks or programs of another.

5        (Source: P.A. 96-262, eff. 1-1-10; 96-1000, eff. 7-2-10.)

6            (720 ILCS 5/16D-3) (from Ch. 38, par. 16D-3)

7            Sec. 16D-3. Computer Tampering.

8            (a) A person commits the offense of computer tampering when  
9 he knowingly and without the authorization of a computer's  
10 owner, as defined in Section 15-2 of this Code, or in excess of  
11 the authority granted to him:

12            (1) Accesses or causes to be accessed or electronically  
13 hi-jacks a computer or any part thereof, a computer  
14 network, electronic mail, social networking website, or a  
15 program or data;

16            (2) Accesses or causes to be accessed or electronically  
17 hi-jacks a computer or any part thereof, a computer  
18 network, electronic mail, social networking website, or a  
19 program or data, and obtains data or services;

20            (3) Accesses or causes to be accessed or electronically  
21 hi-jacks a computer or any part thereof, a computer  
22 network, electronic mail, social networking website, or a  
23 program or data, and damages or destroys the computer or  
24 alters, deletes or removes a computer program or data;

25            (4) Inserts or attempts to insert a "program" into a

1 computer or computer program knowing or having reason to  
2 believe that such "program" contains information or  
3 commands that will or may damage or destroy that computer,  
4 or any other computer subsequently accessing or being  
5 accessed by that computer, or that will or may alter,  
6 delete or remove a computer program or data from that  
7 computer, or any other computer program or data in a  
8 computer subsequently accessing or being accessed by that  
9 computer, or that will or may cause loss to the users of  
10 that computer or the users of a computer which accesses or  
11 which is accessed by such "program"; ~~or~~

12 (5) Falsifies or forges electronic mail transmission  
13 information or other routing information in any manner in  
14 connection with the transmission of unsolicited bulk  
15 electronic mail through or into the computer network of an  
16 electronic mail service provider or its subscribers; or ~~or~~

17 (6) Accesses or causes to be accessed or electronically  
18 hi-jacks a computer or any part thereof, a computer  
19 network, electronic mail, social networking website, or a  
20 program or data, and transmits, sends, or posts false data  
21 such as information, pictures, or videos as the  
22 corresponding account or equipment owner.

23 (a-5) It shall be unlawful for any person knowingly to  
24 sell, give, or otherwise distribute or possess with the intent  
25 to sell, give, or distribute software which (1) is primarily  
26 designed or produced for the purpose of facilitating or

1 enabling the falsification of electronic mail transmission  
2 information or other routing information; (2) has only a  
3 limited commercially significant purpose or use other than to  
4 facilitate or enable the falsification of electronic mail  
5 transmission information or other routing information; or (3)  
6 is marketed by that person or another acting in concert with  
7 that person with that person's knowledge for use in  
8 facilitating or enabling the falsification of electronic mail  
9 transmission information or other routing information.

10 (a-10) For purposes of subsection (a), accessing a computer  
11 network is deemed to be with the authorization of a computer's  
12 owner if:

13 (1) the owner authorizes patrons, customers, or guests  
14 to access the computer network and the person accessing the  
15 computer network is an authorized patron, customer, or  
16 guest and complies with all terms or conditions for use of  
17 the computer network that are imposed by the owner; or

18 (2) the owner authorizes the public to access the  
19 computer network and the person accessing the computer  
20 network complies with all terms or conditions for use of  
21 the computer network that are imposed by the owner.

22 (b) Sentence.

23 (1) A person who commits the offense of computer  
24 tampering as set forth in subsection (a)(1), (a)(5), or  
25 (a-5) of this Section shall be guilty of a Class B  
26 misdemeanor.

1           (2) A person who commits the offense of computer  
2 tampering as set forth in subsection (a) (2) of this Section  
3 shall be guilty of a Class A misdemeanor and a Class 4  
4 felony for the second or subsequent offense.

5           (3) A person who commits the offense of computer  
6 tampering as set forth in subsection (a) (3), ~~or subsection~~  
7 (a) (4), or (a) (6) of this Section shall be guilty of a  
8 Class 4 felony and a Class 3 felony for the second or  
9 subsequent offense.

10           (4) If the injury arises from the transmission of  
11 unsolicited bulk electronic mail, the injured person,  
12 other than an electronic mail service provider, may also  
13 recover attorney's fees and costs, and may elect, in lieu  
14 of actual damages, to recover the lesser of \$10 for each  
15 and every unsolicited bulk electronic mail message  
16 transmitted in violation of this Section, or \$25,000 per  
17 day. The injured person shall not have a cause of action  
18 against the electronic mail service provider that merely  
19 transmits the unsolicited bulk electronic mail over its  
20 computer network.

21           (5) If the injury arises from the transmission of  
22 unsolicited bulk electronic mail, an injured electronic  
23 mail service provider may also recover attorney's fees and  
24 costs, and may elect, in lieu of actual damages, to recover  
25 the greater of \$10 for each and every unsolicited  
26 electronic mail advertisement transmitted in violation of

1           this Section, or \$25,000 per day.

2           (6) The provisions of this Section shall not be  
3           construed to limit any person's right to pursue any  
4           additional civil remedy otherwise allowed by law.

5           (c) Whoever suffers loss by reason of a violation of  
6           subsection (a)(4) of this Section may, in a civil action  
7           against the violator, obtain appropriate relief. In a civil  
8           action under this Section, the court may award to the  
9           prevailing party reasonable attorney's fees and other  
10          litigation expenses.

11          (Source: P.A. 95-326, eff. 1-1-08; 96-1000, eff. 7-2-10.)